Livre blanc

La cybersécurité des plates-formes RBX1 et MBX1

Sommaire

© OMICRON 2021

La cybersécurité des plates-formes RBX1 et MBX1

Les plates-formes matérielles RBX1 et MBX1 ont toutes deux été développées sur la base d'une approche de sécurité intégrée et satisfont aux demandes les plus strictes en matière de cybersécurité et d'intégrité. Des mesures de sécurité appropriées ont été mises en œuvre aux niveaux matériels, logiciels et des processus afin de renforcer le processus de développement, les produits eux-mêmes et le processus de production face aux cybermenaces. Les deux plates-formes et le processus de développement (le cycle de vie de développement logiciel sécurisé) sont actuellement en cours de certification selon la norme CEI 62443.

Mesures de cybersécurité pour le RBX1 et le MBX1

Processus de développement	Matériel et logiciel	Processus de production
Intégration de la cybersécurité au niveau de l'entreprise	Cryptoprocesseur sécurisé	Stockage sécurisé des clés et certificats
Mise en œuvre sécurisée	Démarrage sécurisé et mesuré	Processus strict d'initialisation
Tests de sécurité	Cryptage complet du disque	Entretien sécurisé des équipements
Gestion des vulnérabilités	Mise à jour authentifiées et cryptées	
Certification CEI 62443 en cours	Accès sécurisé à des fins d'assistance et de	
	Principe des moindres privilèges	
	Isolation efficace du PC du poste	
	Certification CEI 62443 en cours	

Ce livre blanc étudie les différentes mesures de cybersécurité introduites dans la conception et le développement continu du RBX1 et du MBX1.

Mesures aux niveaux matériels et logiciels

Des composants matériels de pointe et un logiciel intégré spécialement renforcé sont utilisés pour protéger le RBX1 et le MBX1.

1 Cryptoprocesseur sécurisé

Les deux équipements sont dotés d'une puce de module de plate-forme sécurisée séparée (TPM 2.0) conforme à la norme ISO/CEI 11889. La puce génèrera et stockera en toute sécurité les certificats cryptographiques, et prend en charge le démarrage sécurisé (voir la section 2). Certains certificats sont stockés sur cette puce pendant le processus de production sécurisé (voir la section 13). La puce génère également des clés uniques, utilisées pour crypter les données sur l'équipement (voir la section 3).

© OMICRON 2021

2 Démarrage sécurisé et mesuré

Le RBX1 et le MBX1 utilisent une interface de firmware extensible unifiée (UEFI) moderne spécialement conçue pour OMICRON. Cette interface prend en charge le démarrage sécurisé. Les mécanismes de démarrage sécurisé et mesuré mettent en œuvre les processus de démarrage des équipements, ce qui évite toute exécution de logiciel ou code inconnu sur un équipement. Chaque étape du processus de démarrage contrôle la signature de la phase suivante du processus avant son exécution, pour s'assurer que le RBX1 et le MBX1 ne chargent et n'exécutent que le logiciel qui a été signé par OMICRON. De plus, la fonction de démarrage sécurisé surveille le matériel et le logiciel utilisés par les équipements. En cas de changement détecté, toutes les données de l'équipement restent cryptées et l'équipement ne démarrera pas.

3 Cryptage complet du disque

Toutes les données critiques du RBX1 et du MBX1 sont cryptées et ne peuvent être décryptées que par l'équipement auquel elles sont affectées. La clé utilisée pour crypter les données est générée dans la cryptopuce du RBX1 et du MBX1 (voir la section 1). Ni un tiers ni OMICRON ne peuvent décrypter les données, même si le disque dur est installé dans un MBX1 ou RBX1 différent. Si les équipements détectent une manipulation du contenu du disque dur au cours du démarrage, ils ne démarreront pas. Si, par exemple, le code de cryptage d'un équipement a été compromis, cela n'aura aucun effet sur les données clients d'un autre équipement. Une nouvelle clé ne peut être générée que par une réinitialisation en usine, qui requiert un accès physique à l'équipement.

4 Mises à jour authentifiées et cryptées du firmware

Les mises à niveau du firmware du RBX1 et du MBX1 sont signées à l'aide d'un certificat OMICRON (SHA512). Cela garantit l'authenticité et l'intégrité du fichier de mise à jour du firmware. Pour empêcher toute opération d'ingénierie inverse, les fichiers de mise à jour du firmware sont également cryptés à l'aide du mécanisme de cryptage AES-256-CBC. Les clés nécessaires au décryptage et au contrôle de signature du fichier de mise à jour du firmware sont conservées en toute sécurité sur la puce du cryptoprocesseur (TPM 2.0).

5 Accès sécurisé à des fins d'assistance et de réparation

Le firmware et le matériel ne contiennent aucun mot de passe par défaut ou autre porte dérobée. L'accès au RBX1 et au MBX1 à des fins de maintenance ne peut être accordé que temporairement (la session prend automatiquement fin après un redémarrage) et exige un accès physique en appuyant sur le bouton de réinitialisation situé à l'arrière de l'équipement. Une procédure de défi-réponse, plutôt qu'un mot de passe, permet d'accorder l'accès. L'employé OMICRON doit résoudre un problème cryptographique pour obtenir un accès unique à l'équipement. Ce problème ne peut être résolu qu'à l'aide de l'infrastructure de clés OMICRON (voir la section 12). Il n'y a donc aucun mot de passe par défaut ni aucune clé générale susceptibles de tomber entre de mauvaises mains.

6 Exécution de tous les processus avec des privilèges moindres

Toutes les fonctions critiques du RBX1 et du MBX1 sont réparties entre différents processus. Chaque processus est exécuté avec le niveau de privilèges le moins élevé nécessaire à ses tâches, selon le principe des moindres privilèges. Aucun processus n'a de privilège administrateur.

7 Isolation efficace du PC Windows du poste

Un (ou plusieurs) PC Windows exécutant StationScout, IEDScout ou StationGuard et connecté(s) au RBX1 ou au MBX1 n'exécutent que les fonctions de visualisation et d'interface utilisateur. Toutes les autres fonctions sont réalisées par le firmware sécurisé à l'intérieur de l'équipement. Le RBX1/MBX1 ne transfère aucune donnée entre les ports réseau du poste et ceux du contrôleur. Dans toutes les applications logicielles compatibles, la communication avec l'équipement est authentifiée et cryptée à l'aide du protocole TLS 1.3. StationScout et StationGuard n'acceptent des connexions qu'aux équipements pouvant fournir le certificat de sécurité approprié. Les deux équipements peuvent également isoler le PC de pilotage et le réseau du poste aux niveaux protocolaire et du système d'exploitation. Un PC Windows potentiellement infecté reste donc efficacement isolé du réseau du poste.

© OMICRON 2021

Mesures au sein du processus de développement logiciel

OMICRON a créé un environnement logiciel sécurisé pour le développement de son logiciel et de son firmware, qui garantit une norme constamment élevée en termes de cybersécurité dans le processus de développement. Outre une formation en sécurité, une mise en œuvre sécurisée et une assurance qualité en matière de cybersécurité, le processus couvre également la détection et la gestion des mesures et vulnérabilités potentielles associées à un produit donné. Le cycle de vie de développement logiciel sécurisé repose sur plusieurs normes éprouvées, telles que CEI 62443-4-1, ISO 27000 et NIST 800-30r1, et s'assure que diverses mesures de sécurité ne sont pas ignorées au cours du processus de développement. Il décrit chaque phase du processus, ainsi que les mesures de sécurité standardisées et les bonnes pratiques utilisées.

8 Intégration de la cybersécurité au niveau de l'entreprise

Le cycle de vie de développement logiciel sécurisé garantit également que chaque développement logiciel chez OMICRON répond aux normes de cybersécurité applicables. Le processus débute par une analyse du contexte d'utilisation du produit et une définition des exigences de cybersécurité, avec une modélisation approfondie des risques. La mise en œuvre sécurisée repose sur des normes établies et est constamment vérifiée par les tests de sécurité. Toutes les étapes du processus de développement sont documentées et revérifiées à la fin pour s'assurer que le niveau de sécurité est atteint.

9 Mise en œuvre sécurisée

Des contrôles de sécurité sont réalisés tout au long de la phase de mise en œuvre pour minimiser les soucis de sécurité. Cela implique l'extension de mesures préventives, telles que le respect des directives en matière de sécurisation des codes de programmation, par un examen minutieux du code dans des boucles de révision distinctes. Les douze principes de sécurité devant actuellement être respectés comprennent, par exemple, une réduction de la surface d'attaque en minimisant le nombre d'interfaces ouvertes, le principe susmentionné des moindres privilèges et la résolution des vulnérabilités identifiées dans toute la base de code.

10 Tests de sécurité

Outre la surveillance de la mise en œuvre, le cycle de vie de développement logiciel sécurisé contrôle également les tests de sécurité. Il vérifie si les exigences spécifiées et le niveau de cybersécurité souhaité ont été atteints. La pratique habituelle à cette fin consiste à vérifier le code du programme, à tester la sécurité dynamique et statique de l'application, à surveiller la sécurité de l'application et à analyser la composition du logiciel. Ce dernier point implique, chaque semaine, un examen automatisé minutieux des composants et des vulnérabilités de chaque ligne de code. Les vulnérabilités identifiées doivent ensuite être analysées et résolues par l'équipe de développement. Sur les plates-formes RBX1 et MBX1, des tests de pénétration sont également utilisés pour identifier toute vulnérabilité cachée en matière de sécurité.

11 Gestion des vulnérabilités

Chez OMICRON, chaque type de vulnérabilité en matière de sécurité qui affecte nos produits est pris très au sérieux, et c'est pourquoi nous apprécions tout commentaire pouvant nous aider à améliorer la sécurité de nos produits. OMICRON a donc mis en place une procédure systématique pour l'envoi, la gestion et la communication des vulnérabilités en matière de sécurité. Pour plus de détails sur la procédure de traitement et de communication des vulnérabilités de sécurité des produits OMICRON, consultez le site https://www.omicronenergy.com/security.

© OMICRON 2021

Mesures au sein du processus de production

Outre le processus de développement logiciel, les procédures au cours de la production du matériel RBX1 et MBX1 et leur initialisation ont également été étudiées et adaptées.

12 Stockage sécurisé des clés et certificats

La gestion sécurisée des clés et certificats forme le point central de toutes les autres mesures de sécurité. Le processus de développement sécurisé et les certificats et clés dans nos produits sont générés et gérés via une infrastructure sécurisée. Cette infrastructure essentielle repose sur des modules de sécurité matérielle qui se situent dans des salles de serveur sécurisées. Les modules empêchent l'extraction des clés. Les clés privées d'OMICRON ont été générées dans ce matériel et ne peuvent être extraites, ce qui signifie que même les employés d'OMICRON n'y ont pas accès. Toutes les clés et signatures associées, par exemple pour les mises à jour du firmware, sont générées directement par le matériel à l'aide d'un service spécial. Seul un nombre très limité d'utilisateurs est autorisé à utiliser ce service de signature, et il n'a accès qu'aux services essentiels à ses besoins. La solution va même plus loin en auto-détruisant le module de sécurité matérielle en cas de tentative d'ouverture forcée.

13 Processus strict d'initialisation

Les équipements sont initialisés via une étape de processus ininterrompue que seuls des employés spécifiquement habilités peuvent effectuer. Au cours de ce processus, les clés et certificats cryptographiques sont stockés en toute sécurité sur la puce TPM 2.0. Les employés concernés ont suivi une formation ciblée sur les menaces de cybersécurité et ont parfaitement conscience de tous les aspects de la sécurité des données en entreprise et lors de leurs échanges avec des personnes externes.

14 Entretien sécurisé des équipements

L'équipement est réinitialisé avant toute tâche de réparation. Ceci garantit qu'il ne contient plus aucune donnée client ni information relative à la sécurité. Une fois l'équipement réparé, le processus d'initialisation sécurisée est répété, après quoi les techniciens OMICRON perdent tout droit d'accès. Un renouvellement de l'accès n'est possible que si le client émet à nouveau son fichier de défi (voir la section 5).

Respect des exigences les plus strictes en matière de sécurité

Toutes les mesures mises en œuvre sur les plates-formes RBX1 et MBX1 et dans les applications StationScout et StationGuard sont réévaluées à des intervalles prédéfinis dans le cadre d'un processus d'amélioration continue. Cela garantit que tous les produits continueront à satisfaire aux exigences les plus strictes en termes de cybersécurité et d'intégrité.

© OMICRON 2021

OMICRON travaille avec passion sur des idées innovantes visant à rendre les systèmes énergétiques plus sûrs et plus fiables. Avec nos solutions innovantes, nous faisons face aux défis actuels et futurs de notre secteur. Nous sommes pleinement engagés dans le soutien de nos clients : nous considérons leurs besoins avec sérieux, leur offrons une assistance sur site exceptionnelle et partageons notre expertise et notre expérience.

Le groupe OMICRON développe des technologies innovantes pour tous les domaines de systèmes d'énergie électrique. Les tests électriques d'équipements moyenne et haute tension, les tests de protection, les tests des postes numériques et la cybersécurité sont au cœur de nos activités. Des clients du monde entier font confiance à nos solutions conviviales et apprécient leur précision, leur rapidité et leur qualité.

Nous opérons dans le secteur de l'énergie électrique depuis 1984 et pouvons nous targuer de nombreuses années d'expérience approfondie dans le secteur. Près de 900 employés sur 26 sites apportent leur assistance à nos clients dans plus de 160 pays. Notre équipe d'assistance technique est disponible par téléphone 24 h/24 et 7 jours/7.

Pour plus d'informations, une vue d'ensemble de la documentation disponible et les coordonnées détaillées de nos bureaux dans le monde, consultez notre site Web.

www.omicronenergy.com